UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,569	12/18/2001	Adrian Filipi-Martin	CHM02	2687

7590 08/10/2005

FLINT & KIM, P.A.
P.O. BOX 10827
Greenville, SC 29603

EXAMINER	
ELMORE, JOHN E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,569	FILIPI-MARTIN ET AL.	
	Examiner	Art Unit	
	John Elmore	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Objections

2. **Claim 2 is objected to** because of the following informalities:

the term "a said second request" presumably should read "a second request".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1, 7, 12 and 18 are rejected under 35 U.S.C. 102(b)** as being anticipated by Richard et al. (US 5,922,074), hereafter Richard.

Regarding claim 1, Richard discloses a system for storing and publishing encryption keys for an electronic encryption system that sends encrypted transmissions between a sender and a recipient (col. 2, lines 1-15; col. 6, lines 41-43) comprising:

a first computer readable medium connection for electronic communications over a network having a first communications (Fig. 1 and 2; server 42);

a first storage area embodied within said first computer readable medium (directory database 50);

a second computer readable medium having a second communications connection for electronic communications over a network for providing electronic communications with said first computer readable medium (other directory server accessible by the network; col. 6, lines 51-52);

a second database having a second set of public keys embodied in said second computer readable medium (directory database within other directory server);

a first set of computer readable instructions embodied within said first computer readable medium for:

receiving a request for a recipient's public key from the sender (client 40) through said first communications connection (col. 6, lines 32-48);

querying said first storage area for the requested recipient's public key (col. 6, lines 46-48);

transmitting the recipient's public key to the sender if the recipient's public key is found within said first storage area (col. 6, lines 46-48); and

transmitting a second request for the recipient's public key to said second computer readable medium if the recipient's public key is not found in said first storage area so that the sender is either provided with the recipient's public key or said second request is sent to said second computer readable medium requesting the recipient's public key (col. 6, lines 46-55).

Regarding claim 7, Richard teaches all the limitations of claim 1, and further teaches that said first set of computer readable instructions includes instruction for:

receiving the recipient's public key from said second computer readable medium if the recipient's public key is found within said second database (col. 6, lines 46-48 and 54-55); and,

transmitting the recipient's public key to the sender if the recipient's public key is received from said second computer readable medium so that the sender may encrypt a transmission with the recipient's public key (public key transmitted to sender (as the originating client) after a chain of requests, which allows sender to encrypt a transmission with the public key; col. 6, lines 40-43 and 51-55).

Regarding claims 12 and 18, these are other versions of the claimed system above (claim 1). Therefore, for the reasons provided above, such a claim also is anticipated.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 2-6, 13-16 and 19 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Richard in view of Donnelly ("Designing and LDAP Directory Tree," May 2000).

Regarding claim 2, Richard teaches all the limitations of claim 1, and further teaches that:

said second communications connection allows for electronic communications with a third server (chain of servers; col. 6, line 51-52); and

a second set of computer readable instructions embodied within said second computer readable medium for:

receiving a second request for the recipient's public key from said first set of computer readable instructions (first server 44 forwards request to second server in a chain of servers; col. 6, lines 51-55);

querying said second database for the recipient's public key (col. 6, lines 46-48);

transmitting the recipient's public key to said first computer readable medium if the recipient's public key is found in said second database (col. 6, lines 46-48);

transmitting an upstream request to said third server for the recipient's public key is not found in said second database (second server forwards request to third server in a chain of servers; col. 6, lines 51-55),

receiving the recipient's public key if the recipients' public key is provided by said third server (col. 6, lines 46-48),

receiving a pointer to the recipient's public key if the pointer to the public key is provided by said third server (receive referral (pointer) indicating location where server may be found that can adequately respond to request; col. 6, lines 48-51), and

retrieving the recipient's public key from a location provided by the third server pointer to the recipient's public key if the pointer to the recipient's public key is provided to said first computer readable medium (referred server responds to request by sending recipient's public key; col. 6, lines 46-48).

But Richard does not explicitly explain that the third server is a root server.

However, Donnelly teaches a system for distributing directory services via a directory tree comprising a first directory server (a leaf node on the bottom level of tree), a second directory server (a leaf node on the middle level of tree), and a third directory server (root), wherein the third directory server is a root server, for the purpose of logically grouping information in a manner that increases security and scalability (three-level directory tree; page 1).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Richard with the teaching of Donnelly to provide that the third server is a root server. One would be motivated to do so in order to increase security and scalability by logically grouping information in a tree structure.

Regarding claim 3, the modified system of Richard and Donnelly is referred to as applied to claim 2, and Richard and Donnelly further teach:

a root computer readable medium having a root communications connection for communicating with the network and said second computer readable medium (directory servers connected to each other via network; Richard: Fig. 1; col. 5, lines 7-17; col. 6, lines 24-27);

a root database (directory database 50) embodied in said root computer readable medium a root database embodied in said root computer readable medium containing pointers to all public keys of the encryption system (root is starting point for the entire directory, so it is inherent that root will contain a pointer to all public keys in the directory; Donnelly: page 1);

a set of computer readable root instructions embodied in said root computer readable medium for:

receiving said upstream request from said second set of computer readable instructions (second server forwards request to root server in a chain of servers; Richard: col. 6, lines 51-55),

querying said root database for the pointer to the recipient's public key (Richard: col. 6, lines 46-48),

transmitting the pointer of the recipient's public key to said second computer readable medium if the pointer to the recipient's public key is found within said root database (transmit referral (pointer) indicating location where server may be found that can adequately respond to request; Richard: col. 6, lines 48-51).

But Richard and Donnelly do not explicitly explain a set of computer readable root instructions embodied in said root computer readable medium for transmitting a not found statement to said second computer readable medium if the pointer to the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

However, the Examiner takes official notice that one of ordinary skill in the art would recognize transmitting a not found statement where all other responses to a request have been eliminated for the motivation of maintaining efficiency, integrity and security. That is, where a requested public key is not in the directory, providing an incorrect public key or pointer will jeopardize system efficiency, integrity and security, and providing no response at all will jeopardize system efficiency, as the requesting client may waste time in a wait state pending an expected response. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide for a set of computer readable root instructions embodied in said root computer readable medium for transmitting a not found statement to said second computer readable medium if the pointer to the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

Regarding claim 4, the modified system of Richard and Donnelly is referred to as applied to claim 3, and Richard and Donnelly further teach that said set of computer readable root instructions includes instruction for transmitting said key server address of the next key computer readable medium down the hierarchy having a pointer to the recipient's public key (it is inherent in a directory tree that the root server points to a server down the tree hierarchy; and the referral (pointer) identifies the location (address) of a server on the network; Richard: col. 6, lines 48-51).

Regarding claim 5, the modified system of Richard and Donnelly is referred to as applied to claim 3, and Richard and Donnelly further teach that

a plurality of key computer readable mediums arranged in a hierarchy having public keys stored within said computer readable mediums (directory tree of servers, each storing public keys; Richard: col. 6, lines 41-45; Donnelly: page 1);

a plurality of key server addresses associated with each of said key computer readable mediums representing the location of said key computer readable mediums within said hierarchy (it is inherent in a directory tree that a server points to the location of a plurality of other servers, one up the tree hierarchy and – for non-terminal nodes – one or more down the tree hierarchy; Richard: col. 6, lines 48-51); and,

said set of computer readable root instructions includes instruction for said set of computer readable root instructions includes instruction for transmitting said key server address of the next key computer readable medium down the hierarchy having the recipient's public key (it is inherent that in a directory tree where the server points to the servers that extend down from it in the tree hierarchy, the server points down the hierarchy to the server having the recipient's public key; and the referral (pointer) identifies the location (address) of a server on the network; Richard: col. 6, lines 48-51).

Regarding claim 6, the modified system of Richard and Donnelly is referred to as applied to claim 2, and Richard and Donnelly further teach

a root server cluster having a root computer readable medium and a root communications connection for communicating with the network and said second computer readable medium (directory tree of servers, starting with root, connected by network; Richard: col. 6, line 51-52; Donnelly: page 1);

a root database (directory database 50) embodied within said root server cluster containing pointers to all of the public keys of the encryption system (root is starting point for the entire directory, so it is inherent that root will contain a pointer to all public keys in the directory; Donnelly: page 1);

a set of computer readable medium root instructions embodied in said root server cluster for:

receiving said upstream request from said second set of computer readable instructions (second server forwards request to root server in a chain of servers; Richard: col. 6, lines 51-55),

querying said root database for the requested recipient's public key (Richard: col. 6, lines 46-48),

transmitting the recipient's public key to said second computer readable medium if the recipient's public key is found within said root database (col. 6, lines 46-48).

But Richard and Donnelly do not explicitly explain a set of computer readable root instructions embodied in said root computer readable medium for transmitting a not found statement to said second computer readable medium if the pointer to the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

However, the Examiner takes official notice that one of ordinary skill in the art would recognize transmitting a not found statement where all other responses to a request have been eliminated for the motivation of maintaining efficiency, integrity and

security. That is, where a requested public key is not in the directory, providing an incorrect public key or pointer will jeopardize system efficiency, integrity and security, and providing no response at all will jeopardize system efficiency, as the requesting client may waste time in a wait state pending an expected response. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to provide for a set of computer readable root instructions embodied in said root computer readable medium for transmitting a not found statement to said second computer readable medium if the pointer to the recipient's public key is not found in said root database so that the sender can be provided with the recipient's public key or the sender can be informed that the recipient's public key can not be found.

Regarding claims 13-16 and 19, this is another system version of the claimed system above (claims 2-6). Therefore, for the reasons provided above, such claims also would have been obvious.

6. **Claims 8-11, 17, 20 and 21 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Richard in view of Donnelly and further in view of Knight et al. ("Cashing in on Caching," 1996), hereafter Knight.

Regarding claim 8, Richard teaches all the limitations of claim 7, but does not explain that said first set of computer readable instructions includes instruction for storing the recipient's public key within said first computer readable medium upon receipt of the recipient's public key so that the recipient's public key is available upon subsequent requests received for the recipient's public key.

However, Knight teaches a first computer readable medium (cache server) that includes instruction for storing a client's request in a temporary storage section (cache) within said first computer readable medium upon receipt of the answer so that the answer is available upon subsequent requests for the purpose of improving responsiveness and reducing network load (pages 1 and 2). One of ordinary skill in the art would recognize that a storing the requested public key at the first server would reduce the time and network load required to provide the public key on subsequent requests by the sender.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Richard with the teaching of Knight to provide that said first set of computer readable instructions includes instruction for storing the recipient's public key within said first computer readable medium upon receipt of the recipient's public key so that the recipient's public key is available upon subsequent requests received for the recipient's public key. One would be motivated to do so in order to reduce the time required to respond and the network load.

Regarding claim 9, this is the same as claim 8 with the additional limitation that the first computer readable medium stores the recipient's public key in a temporary storage section (cache; Knight: page 1). Therefore, for reasons provided above, such a claim also would have been obvious.

Regarding claim 10, Richard teaches all the limitations of claim 9, but does not explain that said first set of computer readable instructions include instruction for

deleting the received recipient's public key from said temporary storage section upon the expiration of a predetermined period of time.

However, Knight teaches a first set of computer readable instructions (cache server instructions) include instruction for deleting the received answer from said temporary storage section upon the expiration of a predetermined period of time for the purpose of properly handling short-lived documents (page 3). One of ordinary skill in the art would recognize that recipient's public key is equivalent to a short-lived document in that it may change or expire after a predetermined time.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Richard with the teaching of Knight to provide for a first set of computer readable instructions include instruction for deleting the received answer from said temporary storage section upon the expiration of a predetermined period of time for the purpose of handling short-lived documents. One would be motivated to do so in order to properly handle public keys that may change or expire within a predetermined time.

Regarding claim 11, this is essentially the same as claim 10 with the exception that the recipient's public key is deleted according to a set of predetermined criteria. One of ordinary skill in the art would recognize that a predetermined time qualifies as set of predetermined criteria. Therefore, for the reasons provided above in claim 10, such a claim also would have been obvious.

Regarding claims 17, 20 and 21, these are other versions of the claimed system above (claims 8-11). Therefore, for the reasons provided above, such a claim also would have been obvious.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Svrivastava (US 6,684,331) discloses a method for distributing cryptographic keys over a network using a tree structure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John Elmore whose telephone number is 571-272-4224. The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JE

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100